

RECEIVED
CENTRAL FAX CENTER

APR 14 2005

**Yee &
Associates, P.C.**4100 Alpha Road
Suite 1100
Dallas, Texas 75244Main No. (972) 385-8777
Facsimile (972) 385-7766**Facsimile Cover Sheet**

To: Commissioner for Patents for Examiner Niles R. Shah Group Art Unit 2127	Facsimile No.: 703/872-9306
From: Lourdes Perez for Carrie Parker Legal Assistant to Vicky Ash	No. of Pages Including Cover Sheet: 33
Message: Enclosed herewith: <ul style="list-style-type: none">• Transmittal Document; and• Appeal Brief.	
Re: Application No. 09/353,974 Attorney Docket No: AT9-99-123	
Date: Thursday, April 14, 2005	
Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	<i>This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.</i>

**PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY
FAXING A CONFIRMATION TO 972-385-7766.**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Berstis et al.**Serial No.: **09/353,974**Filed: **July 15, 1999**For: **Method and System for
Encryption of Web Browser Cache****35525**PATENT TRADEMARK OFFICE
CUSTOMER NUMBER§
§
§
§
§Group Art Unit: **2127**Examiner: **Shah, Nilesh R.**Attorney Docket No.: **AT9-99-123**Certificate of Transmission Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on April 14, 2005.

By:


Lourdes PerezTRANSMITTAL DOCUMENTCommissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

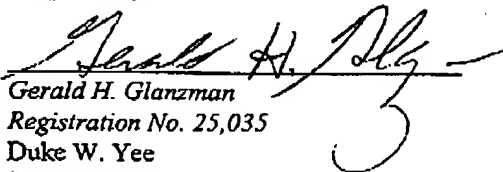
Sir:

ENCLOSED HERewith:

- Appeal Brief (37 C.F.R. 41.37).

A fee of \$500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,


Gerald H. Glanzman
Registration No. 25,035
Duke W. YeeRegistration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER

APR 14 2005

Docket No. AT9-99-123

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Berstis et al.**

Serial No.: **09/353,974**

Filed: **July 15, 1999**

For: **Method and System for
Encryption of Web Browser Cache**

§
§
§
§
§
§
§
§

Group Art Unit: **2127**

Examiner: **Shah, Nilesb R.**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via
facsimile to the Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450, facsimile number (703) 872-9306
on April 14, 2005.

By:


Lourdes Perez

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on February 14, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

(Appeal Brief Page 1 of 31)
Berstis et al. - 09/353,974

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-21

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-21
4. Claims allowed: NONE
5. Claims rejected: 1-21
6. Claims objected to: NONE

C. CLAIMS ON APPEAL

The claims on appeal are: 1-21

STATUS OF AMENDMENTS

No amendments were made in the Response to Office Action, dated July 22, 2004 or after the Final Office Action dated November 12, 2004.

SUMMARY OF CLAIMED SUBJECT MATTER**A. CLAIM 1 - INDEPENDENT**

The subject matter of claim 1 is directed to a method in a data processing system (100, 200 and 300) for securing information stored in a browser cache associated with a browser (400, 500, 600, 700, 800 and 900). A session is initiated and a first web page (422, 510) is requested. The requested web page (422, 510) is received (step 1102). The received web page (422, 510) is encrypted (steps 1108 and 1112 or step 1110) (see *Specification*, page 5, lines 14-17 and page 27, line 19 through page 28, line 12; and **Figures 8 and 11**). Then, the encrypted web page is cached (step 1114). As the user browses network nodes or web pages (422, 510) on a network, the browser encrypts the web pages (steps 1110 and 1112) before the web pages are cached (step 1114) (see *Specification*, page 5, lines 19-21 and **Figure 11**) to secure the information stored in the browser cache associated with the browser.

B. CLAIM 9 - INDEPENDENT

The subject matter of claim 9 is directed to a method in a data processing system (100, 200 and 300) for securing information stored in a browser cache. An application is opened using a browser (400, 500, 600, 700, 800 and 900). An application specific function is performed on the application using the browser producing application specific information. The produced application specific information is encrypted (steps 1108 and 1112 or step 1110) (see *Specification*, page 5, lines 14-17 and page 27, line 19 through page 28, line 12; and **Figures 8 and 11**). Then, the encrypted application specific information is cached (step 1114) (see *Specification*, page 5, lines 19-21 and **Figure 11**) to secure the information stored in the browser cache associated with the browser.

C. CLAIM 10 - INDEPENDENT

The subject matter of claim 10 is directed to a method in a data processing system (100, 200 and 300) for securing information stored in a browser cache associated with a browser (400, 500, 600, 700, 800 and 900). A session is initiated and data associated with information content

stored in the browser cache is decrypted (step 1210). A user requests information that is stored in the browser cache. The decrypted data is checked for the requested information (step 1212). Additional data contained in the browser cache, which is the information requested by the user (step 1202) and stored in the browser cache, is decrypted (steps 1216, 1218 and 1220) (see *Specification*, page 5, lines 21-23 and page 28, line 13 through page 29, line 29; and Figure 12).

D. CLAIM 11 – INDEPENDENT

The subject matter of claim 11 is directed to a data processing system (100, 200 and 300) for securing information stored in a browser cache associated with a browser (400, 500, 600, 700, 800 and 900). The data processing system provides a means for initiating a session and a means for requesting a first web page (422, 510). The data processing system provides a means for receiving the requested web page (422, 510) (step 1102). The data processing system provides a means for encrypting the received web page (422, 510) (steps 1108 and 1112 or step 1110) (see *Specification*, page 5, lines 14-17 and page 27, line 19 through page 28, line 12; and Figures 8 and 11). Then, the data processing system provides a means for caching the encrypted web page (step 1114).

E. CLAIM 19 - INDEPENDENT

The subject matter of claim 19 is directed to a data processing system (100, 200 and 300) for securing information stored in a browser cache. The data processing system provides a means for opening an application using a browser (400, 500, 600, 700, 800 and 900). The data processing system provides a means for performing an application specific function on the application using the browser producing application specific information. The data processing system provides a means for encrypting the produced application specific information (steps 1108 and 1112 or step 1110) (see *Specification*, page 5, lines 14-17 and page 27, line 19 through page 28, line 12; and Figures 8 and 11). Then, the data processing system provides a means for caching the encrypted application specific information (step 1114) (see *Specification*, page 5, lines 19-21 and Figure 11) to secure the information stored in the browser cache associated with the browser.

F. CLAIM 20 - INDEPENDENT

The subject matter of claim 20 is directed to a data processing system (100, 200 and 300) for securing information stored in a browser cache associated with a browser (400, 500, 600, 700, 800 and 900). The data processing system provides a means for initiating a session and an means for decrypting data associated with information content stored in the browser cache (step 1210). The data processing system provides a means for requesting information that is stored in the browser cache. The data processing system provides a means for checking the decrypted data for the requested information (step 1212). The data processing system provides a means for decrypting additional data contained in the browser cache, which is the information requested by the user (step 1202) and stored in the browser cache (steps 1216, 1218 and 1220) (see *Specification*, page 5, lines 21-23 and page 28, line 13 through page 29, line 29; and **Figure 12**).

G. CLAIM 21 - INDEPENDENT

The subject matter of claim 21 is directed to a computer program product on a computer readable medium (100, 200 and 300) for securing information stored in a browser cache associated with a browser (400, 500, 600, 700, 800 and 900). The computer program product provides instructions for initiating a session and instructions for requesting a first web page (422, 510). The computer program product provides instructions for receiving the requested web page (422, 510) (step 1102). The computer program product provides instructions for encrypting the received web page (422, 510) (steps 1108 and 1112 or step 1110) (see *Specification*, page 5, lines 14-17 and page 27, line 19 through page 28, line 12; and **Figures 8 and 11**). Then, the computer program product provides instructions for caching the encrypted web page (step 1114).

H. CLAIM 2 - DEPENDENT

The subject matter of claim 2, which depends from claim 1, is directed to a method of encrypting the web page comprising coding the web page using a browser supported encryption algorithm (see *Specification*, page 21, line 21 through page 22, line 16 and **Figure 8**).

I. CLAIM 3 – DEPENDENT

The subject matter of claim 3, which depends from claim 1, is directed to a method of encrypting the web page comprising coding the web page using an encryption application not supported by the browser (see *Specification*, page 21, line 21 through page 29, line 16 and **Figure 8**).

J. CLAIM 4 – DEPENDENT

The subject matter of claim 4, which depends from claim 1, is directed to a method of encrypting the web page comprising selecting a browser supported encryption algorithm for encrypting the web page (see *Specification*, page 21, line 21 through page 22, line 16 and **Figure 8**).

K. CLAIM 5 – DEPENDENT

The subject matter of claim 5, which depends from claim 1, is directed to a method of caching the web page further comprising providing a remote cache location (see *Specification*, page 23, line 8 through page 25, line 2 and **Figure 9**).

L. CLAIM 6 - DEPENDENT

The subject matter of claim 6, which depends from claim 1, is directed to a method for password protecting the browser and browser cache from unauthorized users (see *Specification*, page 26, line 18 through page 27 line 6 and **Figures 7, 8 and 10**).

M. CLAIM 7 – DEPENDENT

The subject matter of claim 7, which depends from claim 1, is directed to a method of encrypting the web page comprising defining a path for storing the web page that directs the web page to memory locations for encrypted data (see *Specification*, page 23, line 8 through page 24, line 18 and **Figure 9**).

N. CLAIM 8 – DEPENDENT

The subject matter of claim 8, which depends from claim 1, is directed to a method wherein web

page information that is cached and then paged is paged as encrypted web page information (see *Specification*, page 24, line 19 through page 25, line 2 and **Figure 8**).

O. CLAIM 12 – DEPENDENT

The subject matter of claim 12, which depends from claim 11, is directed to a system for encrypting the web page comprising coding the web page using a browser supported encryption algorithm (see *Specification*, page 21, line 21 through page 22, line 16 and **Figure 8**).

P. CLAIM 13 – DEPENDENT

The subject matter of claim 13, which depends from claim 11, is directed to a system for encrypting the web page comprising coding the web page using an encryption application not supported by the browser (see *Specification*, page 21, line 21 through page 22, line 29 and **Figure 8**).

Q. CLAIM 14 – DEPENDENT

The subject matter of claim 14, which depends from claim 11, is directed to a system for encrypting the web page comprising selecting a browser supported encryption algorithm for encrypting the web page (see *Specification*, page 21, line 21 through page 22, line 16 and **Figure 8**).

R. CLAIM 15 – DEPENDENT

The subject matter of claim 15, which depends from claim 11, is directed to a system for caching the web page further comprising providing a remote cache location (see *Specification*, page 23, line 8 through page 25, line 2 and **Figure 9**).

S. CLAIM 16 – DEPENDENT

The subject matter of claim 16, which depends from claim 11, is directed to a system for password protecting the browser and browser cache from unauthorized users (see *Specification*,

page 26, line 18 through page 27 line 6 and **Figures 7, 8 and 10**).

T. CLAIM 17 – DEPENDENT

The subject matter of claim 17, which depends from claim 11, is directed to a system for encrypting the web page comprising defining a path for storing the web page that directs the web page to memory locations for encrypted data (see *Specification*, page 23, line 8 through page 24, line 18 and **Figure 9**).

U. CLAIM 18 – DEPENDENT

The subject matter of claim 18, which depends from claim 11, is directed to a system wherein web page information that is cached and then paged is paged as encrypted web page information (see *Specification*, page 24, line 19 through page 25, line 2 and **Figure 8**).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL**A. GROUND OF REJECTION 1 (Claims 1-21)**

Claims 1-21 are finally rejected under 35 U.S.C. § 103(a) as being allegedly obvious over *Chang et al.* (U.S. Patent Number 6,105,012), in view of *Sasich et al.* (U.S. Patent Number 6,661,904).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-21)

Claims 1-21 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over *Chang et al.* (U.S. Patent 6,105,012), hereinafter referred to as *Chang*, in view of *Sasich et al.* (U.S. Patent 6,661,904), hereinafter referred to as *Sasich*. This rejection is respectfully traversed.

A.1. Claims 1, 9-11 and 19-21

As to independent claim 1, the Final Office Action states:

As per claim 1, Chang teaches the invention substantially as claimed including the use of a data processing implemented method comprising: initiating a session, requesting a first web page, receiving the web page (col. 4 line 1-20, col. 8 lines 15-20, col. 8 lines 39-45), encrypting the web page (col. 4 lines 20-22, col. 4 lines 61-62, col. 8 lines 43-55) Chang does not teach the use of securing information stored in a cache.

Sasich teaches the use of securing information stored in a cache (col. 7, lines 25-30; col. 7, lines 46-55; col. 13 lines 30-40; col. 14, lines 57-65).

It would have been obvious to one skilled in the art at the time of the invention to combine Chang and Sasich in order to have a secure cache. By having Sasich's secure cache system, a third party may not access information associated the cache (i.e., personal information).

Final Office Action dated November 12, 2004, pages 2-3.

Claim 1, which is representative of the other rejected independent claims 11 and 21 with regard to similarly recited subject matter, reads as follows:

1. A data processing implemented method for securing information stored in a browser cache associated with a browser, the method comprising:
 - initiating a session;
 - requesting a first web page;
 - receiving the web page;
 - encrypting the web page; and
 - caching the web page. (emphasis added)

Claim 9, which is representative of the other rejected independent claim 19 with regard to similarly recited subject matter, reads as follows:

9. A data processing implemented method for securing information stored on a browser cache, the method comprising:
 - opening an application using a browser;

performing an application specific function on the application using the browser, wherein application specific information is produced;
encrypting the application specific information; and
caching the application specific information. (emphasis added)

Claim 10, which is representative of the other rejected independent claim 20 with regard to similarly recited subject matter, reads as follows:

10. A data processing implemented method for securing information stored in a browser cache associated with a browser, the method comprising:
initiating a session;
decrypting data contained in the browser cache, wherein the decrypted data is associated with information content stored in the browser cache;
requesting information stored in the browser cache;
checking the decrypted data for requested information; and
decrypting additional data contained in the browser cache, wherein the decrypted data is the requested information. (emphasis added)

Chang and *Sasich*, taken alone or in combination, do not teach or suggest securing information stored in a browser cache associated with a browser as recited in the steps of independent claims 1, 9-11 and 19-21. The independent claims of the present invention are claimed in the context of "securing information stored in a browser cache associated with a browser." Neither reference, *Chang* nor *Sasich*, addresses this issue. Because neither of the cited references is directed to the problem addressed by the present invention, their combination would not form the invention of claims 1, 9-11 and 19-21, particularly in the context of a browser cache.

Chang is directed to a "security system and method for financial institution server and client web browser." The invention deals with using HTML format to send and receive, between a financial institution server and a client computer with a web browser, forms representing financial transactions. (See Abstract, lines 1-10). According to *Chang*, these forms are encrypted for transit. Though *Chang* is clearly concerned with security, *Chang* does not appear to teach or suggest the idea of encrypting the data to be cached for the purpose of keeping the data secure within the cache. *Chang* appears to be concerned with keeping the data secure during transmission where it is most vulnerable to interception by a hacker, and does not address desirability of protecting received pages at the browser.

Sasich is directed to a method and system for automated electronic conveyance of hidden data. A transformation of a data object called a personal logo contains personal data for

transmitting from a client computer to a server computer. During processing to create a personal logo, a user is prompted for personal information. *Sasich* teaches that the personal information includes a name, an email address, a physical address, a telephone number, a credit card number, a social security number, a mother's maiden name, a personal identification number, a gender, a race, a religion, a disability, a sexual preference, a blood type, an allergy, a measure of income, a hobby, a name of a publication subscribed to, a job title, an injury, a garment size, a weight, an eye color, a fingerprint, a hand geometry, a height, a food preference, a disease, a hair color, a genotype, a voice print, a post office box, a shoe size, an occupation, an accreditation, a date of birth, a date of encoding, a place of birth, a time of encoding, a filename, a universal record locator, an iris code, a retinal code, a license number, a security clearance level, a language, a processor serial number, and an alias. The personal information is deposited in a raw data cache for later combination with a unique graphic personal identifier to form a data conveyance object. The raw data cache itself may be encrypted and stored in an encrypted form. The personal data is embedded into transformation coefficients derived using one of several encoding techniques to hide and make the personal data difficult for an unauthorized party to extract. The personal data is extracted from the transformation coefficients by the server computer to complete the transaction. Thus, *Sasich* may teach encrypting a raw data cache of personal information, but does not teach or suggest securing information stored in a browser cache associated with a browser. Further, *Sasich* does not teach encrypting information received by a browser and then caching the encrypted information in a browser cache.

The Final Office Action points to *Sasich*, stating that "*Sasich* teaches the use of securing information stored in a cache...." The Final Office Action refers to the following portions of *Sasich* at col. 7, lines 25-30 and lines 46-55:

In step 108a, the personal data is deposited in a raw data cache which includes groupings of user specified personal and privacy data and transaction related protocols. Custom data caches may be formed in connection with certain kinds of transactions.

Each raw data cache will be encoded to operate at a designated level of security commensurate with protection appropriate to the kind of data contained within it and required by the anticipated transaction. Raw data cache level 1 may contain basic usernames, email address, and appropriate base level security. Raw data cache level 4 may contain credit card numbers and other sensitive personal financial data requiring higher designated levels of security and verification.

Although the above citations mention encoding the "raw data caches," *Sasich* does not teach this in the context of a browser program, as claimed in claim 1 of the present invention. Instead, *Sasich* is directed to a method of encoding data in an image ("personal logo") for transmission. The above passages do not describe general treatment of data in *Sasich*, but only describe one step in the creation of the personal logo, which is then used to transmit the sensitive data. For example, *Sasich* states at col. 3, lines 1-5:

The present invention makes use of digital graphical bitmaps to establish a visual representation of a sender's identity and authority. Corresponding data streams are used to transmit the sender's identity, authority, and data associated with the sender across a network.

As described in *Sasich*'s detailed description, the caching steps recited by the Final Office Action are not in the context of a browser, and are only one step in the creation of the personal logo, which is a method of encrypting data for transmission. *Sasich* is not directed to protecting cached web pages by encrypting them and caching them, as claimed in claim 1.

Specifically, the passages recited above by Examiner are in the context of Figure 2 of *Sasich*. At col. 5, lines 46-48, *Sasich* starts the discussion of the process:

FIG. 2 shows a methodology for creating a personal logo. To make use of the personal logo capability, the user may first install client software on his or her computer. (emphasis added)

Sasich goes on describing the method of FIG. 2. Step 108a, from which the Final Office Action draws the above cited language, is given in *Sasich* as part of the logo creation process. This differs significantly from the present invention, which is directed to encrypting and caching web pages. In the logo creation process, according to *Sasich* in FIG. 2, the steps include receiving a base image (105); processing it to make the image unique (106); optimizing the image (107); receive data for encoding (108); cache the data (108a); combine the data with the image (109); store the UGPI (110); and display the personal logo (110).

The underlined steps are intended to highlight the fact that *Sasich* is not receiving, encrypting, and caching a web page as claimed. Instead, the step of caching is recited in the context of creating the personal logo, which is used as a means to transmit information securely. Hence, Appellants respectfully submit that the cited language from col. 7 stating, "Each raw data cache will be encoded to operate at a designated level of security commensurate with protection appropriate to the kind of data contained within it..." does not teach the claimed limitations of,

"receiving the web page; encrypting the web page; and caching the web page."

Hence, it is respectfully submitted that the combination of references does not teach the claimed invention. Teaching to encrypt cached data (such as that recited by *Sasich*: name, email address, phone number, etc.) for a specific process to create a personal security logo does not make obvious all uses of encrypted data, especially that taught in the context of claim 1.

Hence, Appellants respectfully submit that the two references, even if properly combined, do not teach or suggest the claimed invention.

Further, the cited references do not mention or suggest the modifications necessary to reach the claimed invention. In order for the two cited references to teach the claimed invention, significant modifications to their teaching would be necessary. For example, the encryption of cached data of *Sasich* would have to be modified to apply to a downloaded web page. Alternately, the teaching of *Chang* would have to be modified to include encryption of cached web pages, which is not taught nor suggested. The mere fact that the prior art could be modified to arrive at the claimed invention does not render the claimed invention obvious; the prior art must suggest the desirability of such a modification. *In re Ochiai*, 71 F.3d 1565, 1570, 37 U.S.P.Q.2d 1127, 1131 (Fed. Cir. 1996); *In re Gordon*, 733 F.2d 900, 903, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984). Merely stating that the modification would have been obvious to one of ordinary skill without identifying an incentive or motivation for making the proposed modification is insufficient to establish a *prima facie* case.

It is also respectfully submitted that neither *Chang* nor *Sasich* specifically addresses the problem of the present invention, namely, protecting cached data in a user's machine that might be accessible to others. For example, the present invention states on page 3, line 29 through page 4, line 4:

Even when the cache is physically located on the user's computer, the user cannot assume that the contents of the disk cache are safe from outside intrusion, much less secure if another user has access to the user's web browser. Anyone having access to the user's web browser cache could conceivably reconstruct a user's web searching activity and deduce the subject matter of the search.

Nothing in *Sasich* nor *Chang* addresses this problem. Hence, it is respectfully submitted that the combination of *Sasich* and *Chang* cannot be properly combined in the way suggested in the Final Office Action. Hence, claim 1 is believed distinguished from the cited references. Likewise, the other independent claims discuss the innovations of the present application in the

context of a browser, and are believed distinguished on the grounds applicable to claim 1, argued above. For these reasons, all independent claims are believed distinguished from the cited references.

Since *Chang* and *Sasich*, taken alone or in combination, do not teach or suggest the features of independent claims 1, 9-11 and 19-21, *Chang* and *Sasich*, taken alone or in combination, do not teach or suggest the features of dependent claims 2-8 and 12-18 at least by virtue of their dependency on claims 1 and 11. Accordingly, Appellants respectfully request withdrawal of the rejection of claims 1-21 under 35 U.S.C. § 103(a).

A.2. Claims 2, 3, 4, 12, 13 and 14

In addition to the above, Appellants respectfully submit that claims 2, 3, 4, 12, 13 and 14 are independently distinguishable from the *Chang* and *Sasich* references. Claims 2 and 12 depend from claims 1 and 11, respectively, and additionally recite that the step of encrypting the web page further comprises coding the web page using a browser supported encryption algorithm. Claims 3 and 13 depend from claims 1 and 11, respectively, and additionally recite that the step of encrypting the web page further comprises coding the web page using an encryption application not supported by the browser. Claims 4 and 14 depend from claims 1 and 11, respectively, and additionally recite that the step of encrypting the web page further comprises selecting a browser supported encryption algorithm for encrypting the web page. The *Chang* and *Sasich* references do not teach or suggest these features.

In the rejection of claims 2, 4, 12 and 14, the Office Action refers to the following portions of *Chang*:

In certain cases, the HTML forms 124a can be transmitted to the web browser 216 in an encrypted format or without any special formatting. The web browser returns messages 143 containing form data to the financial server 102 in an encrypted format, a format containing the user's digital signature and timestamp, an encrypted format containing the user's digital signature and timestamp, or without any special formatting.

Chang, column 4, lines 8-15. (emphasis added)

In accordance with a preferred embodiment, the FORM tag includes special fields that indicate how the associated HTML document is formatted (e.g., whether or not it is encrypted). If the HTML document sent by the server to a client is encrypted, a special "key" field in the FORM tag can be used to specify the server's public key.

Chang, column 11, lines 20-25.

If the requested return message format specified encryption (i.e., `oufformat="encrypt"`), the web browser 216 performs some of the same steps described above. The web browser 216 randomly generates a session key 254 (step 394). The form data is then encrypted with the randomly generated session key 254 (step 396). The session key 254 is affixed to the encrypted form data and encrypted with the server's public key 142 (step 398). A header record 252 is then generated containing a flag 258 having the appropriate value ("E") and the key length 260 of the enclosed session key. The message is formatted and then transmitted to the financial server 102 (step 400).

Chang, column 12, lines 15-25.

These portions of *Chang* only teach that a browser is capable of 1) receiving encrypted data and 2) encrypting a message returned to a financial server. *Chang* does not teach or suggest encrypting a web page in the specific manners described in claims 2, 3, 4, 12, 13 and 14. Therefore, claims 2, 3, 4, 12, 13 and 14 are believed distinguished from the cited references.

A.3. Claims 5 and 15

In addition to the above, Appellants respectfully submit that claims 5 and 15 are independently distinguishable from the *Chang* and *Sasich* references. Claims 5 and 15 depend from claims 1 and 11, respectively, and additionally recite that the step of caching the web page further comprises providing a remote cache location. The *Chang* and *Sasich* references do not teach or suggest this feature.

In the rejection of claims 5 and 15, the Office Action refers to the following portion of *Chang*:

The second new field is the key field (e.g., `key="server's public key"`) which is used to indicate the server's public key. The server's public key is used in the encryption process associated with the returned user registration message.

Chang, column 7, lines 14-17.

This portion of *Chang* only describes the extensions to the HTML form tag. *Chang* does not teach or suggest caching a web page in the specific manner described in claims 5 and 15, namely, by providing a remote cache location. Therefore, claims 5 and 15 are believed distinguished from the cited references.

A.4. Claims 6 and 16

In addition to the above, Appellants respectfully submit that claims 6 and 16 are independently distinguishable from the *Chang* and *Sasich* references. Claims 6 and 16 depend from claims 1 and 11, respectively, and additionally recite that one of the browser and the browser cache is password protected from unauthorized users. No such teaching is found in either reference. In the rejection of claims 6 and 16, the Final Office Action cites *Sasich* at col. 7, lines 45-55 and col. 13 lines 30-47, which state:

Each raw data cache will be encoded to operate at a designated level of security commensurate with protection appropriate to the kind of data contained within it and required by the anticipated transaction. Raw data cache level 1 may contain basic usernames, email address, and appropriate base level security. Raw data cache level 4 may contain credit card numbers and other sensitive personal financial data requiring higher designated levels of security and verification.

As an alternative to creating a base logo based upon user input, a base logo may be provided by a third party such as a web vendor. Whereas a user-selected base logo is useful for many generic network transactions, a third party-provided base logo is useful for encoding information particular to the type of transactions that a user may repeatedly have with that third party. For example, a web-based clothing retailer may wish to encode a user's clothing sizes, color preference, height, weight, hair color, eye color, shoe size, customer number and favorite activities. Such data would be useful for automating ordering transactions and for recommending merchandise to that customer. For the case of a third party-provided base logo, the logo may be a pictorial representation of a vendor's business logo. Such a logo may, after creation, be co-resident on a user's computer with other third party logos representing data useful to other vendors, clubs, special interest groups, employers, unions, banks, utility companies, or other parties with which the user has occasional or regular transactions.

These passages do not teach or suggest the limitations of claims 6 and 16, namely, that a browser cache is password protected. Hence, claims 6 and 16 are believed distinguished from the cited references.

A.5. Claims 7 and 17

In addition to the above, Appellants respectfully submit that claims 7 and 17 are independently distinguishable from the *Chang* and *Sasich* references. Claims 7 and 17 depend from claims 1 and 11, respectively, and additionally recite that the step of encrypting the web page further comprises defining a path for storing the web page that directs the web page to

memory locations for encrypted data. The *Chang* and *Sasich* references do not teach or suggest this feature.

In the rejection of claims 7 and 17, the Office Action refers to the following portions of *Chang*:

The communications interface 112 is used to communicate with other user workstations as well as other system resources not relevant here.

The primary memory 114 of the server computer 102 may be implemented as RAM (random access memory) or a combination of RAM and non-volatile memory such as magnetic disk storage. The primary memory 114 of the server computer 102 can contain the following:

- an operating system 116;
- Internet access procedures 118;
- Web server procedures 120;
- an audit trail 122 tracking each financial transaction processed by the financial server 102;
- an HTML document repository 124;
- an encryption procedure 126 for encrypting and decrypting data;

Chang, column 4, lines 48-60.

The primary memory 208 of the client computer 106 may be implemented as RAM (random access memory) or a combination of RAM and non-volatile memory such as magnetic disk storage. The primary memory 208 of the server computer 102 can contain the following:

- an operating system 210;
 - network access procedures 212;
 - an HTML document repository 214;
 - a web browser 216;
 - messages 143;
 - as well as other data structures and procedures.
- The web browser 216 can contain the following:
- one or more user encryption keys 218 associated with the user's digital signature;
 - an encryption procedure 220 for encrypting and decrypting data;
 - a random key generation procedure 222 for randomly generating session keys;
 - a formatting procedure 224 for configuring a return message in a requested manner;
 - an initialization procedure 226 that establishes the user's encryption keys 218;
 - timestamp procedures 228 that generate a timestamp representing a time and date;
 - digital signature procedures 230 that are used to sign a form and verify a user's digital signature;
 - the user's password 232;
 - a browser welcome web page 234;
 - a browser's encryption key 240 that is used to encrypt the users encryption keys 218;

one or more session keys 241 for use in encrypting return messages to the server; as well as other data structures and procedures.

Chang, column 5, lines 13-45.

These portions of *Chang* only describe the system architecture for *Chang*'s invention. *Chang* does not teach or suggest encrypting a web page in the specific manner described in claims 7 and 17, namely, by defining a path for storing the web page that directs the web page to memory locations for encrypted data. Therefore, claims 7 and 17 are believed distinguished from the cited references.

A.6. Claims 8 and 18

In addition to the above, Appellants respectfully submit that claims 8 and 18 are independently distinguishable from the *Chang* and *Sasich* references. Claims 8 and 18 depend from claims 1 and 11, respectively, and additionally recite that web page information that is cached and then paged is paged as encrypted web page information. The *Chang* and *Sasich* references do not teach or suggest this feature.

In the rejection of claims 8 and 18, the Office Action refers to the following portions of *Sasich*:

Caches can also be distinguished by type of electronic storage technology, for instance hard disk, touch memory, floppy disk, etc., and by types of other software devices used with the data, particularly those performing security and encryption functions.

Sasich, column 7, lines 42-46.

As an alternative to creating a base logo based upon user input, a base logo may be provided by a third party such as a web vendor. Whereas a user-selected base logo is useful for many generic network transactions, a third party-provided base logo is useful for encoding information particular to the type of transactions that a user may repeatedly have with that third party. For example, a web-based clothing retailer may wish to encode a user's clothing sizes, color preference, height, weight, hair color, eye color, shoe size, customer number and favorite activities. Such data would be useful for automating ordering transactions and for recommending merchandise to that customer. For the case of a third party-provided base logo, the logo may be a pictorial representation of a vendor's business logo. Such a logo may, after creation, be co-resident on a user's computer with other third party logos representing data useful to other vendors, clubs, special interest groups, employers, unions, banks, utility companies, or other parties with which the user has occasional or regular transactions.

Sasich, column 13, lines 30-47.

writing each said corresponding transformation coefficients and said reference to said corresponding library block to memory.

Sasich, column 15, lines 25-28.

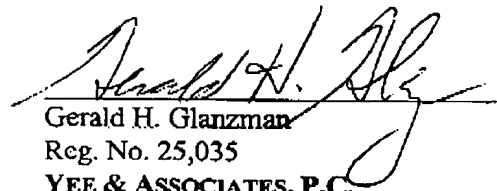
These portions of *Sasich* do not teach or suggest that web page information that is cached and then paged is paged as encrypted web page information, as recited in claims 8 and 18.

Therefore, claims 8 and 18 are believed distinguished from the cited references.

CONCLUSION

In view of the above, Appellants respectfully submit that claims 1-21 define over the prior art of record. Appellants therefore respectfully request the Board of Patent Appeals and Interferences to overturn the rejection of claims 1-21 under 35 U.S.C. 103(a).

Respectfully submitted,



Gerald H. Glanzman

Reg. No. 25,035

YEE & ASSOCIATES, P.C.

PO Box 802333

Dallas, TX 75380

(972) 385-8777

Attorney for Appellants

GHG/vja

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A data processing implemented method for securing information stored in a browser cache associated with a browser, the method comprising:

initiating a session;

requesting a first web page;

receiving the web page;

encrypting the web page; and

caching the web page.
2. The method recited in claim 1, wherein the step of encrypting the web page further comprises coding the web page using a browser supported encryption algorithm.
3. The method recited in claim 1, wherein the step of encrypting the web page further comprises coding the web page using an encryption application not supported by the browser.
4. The method recited in claim 1, wherein the step of encrypting the web page further comprises selecting a browser supported encryption algorithm for encrypting the web page.
5. The method recited in claim 1, wherein the step of caching the web page further comprises providing a remote cache location.

6. The method recited in claim 1, wherein one of the browser and the browser cache is password protected from unauthorized users.
7. The method recited in claim 1, wherein the step of encrypting the web page further comprises defining a path for storing the web page that directs the web page to memory locations for encrypted data.
8. The method recited in claim 1, wherein web page information that is cached and then paged is paged as encrypted web page information..
9. A data processing implemented method for securing information stored on a browser cache, the method comprising:
 - opening an application using a browser;
 - performing an application specific function on the application using the browser, wherein application specific information is produced;
 - encrypting the application specific information; and
 - caching the application specific information.
10. A data processing implemented method for securing information stored in a browser cache associated with a browser, the method comprising:
 - initiating a session;
 - decrypting data contained in the browser cache, wherein the decrypted data is associated with information content stored in the browser cache;

requesting information stored in the browser cache;
checking the decrypted data for requested information; and
decrypting additional data contained in the browser cache, wherein the decrypted data is the requested information.

11. A data processing system for securing information stored in a browser cache associated with a browser, the system comprising:

initiating means for initiating a session;
requesting means for requesting a first web page;
receiving means for receiving the web page;
encrypting means for encrypting the web page; and
caching means for caching the web page.

12. The system recited in claim 11, wherein the encrypting means for encrypting the web page further comprises coding the web page using a browser supported encryption algorithm.

13. The system recited in claim 11, wherein the encrypting means for encrypting the web page further comprises coding the web page using an encryption application not supported by the browser.

14. The system recited in claim 11, wherein the encrypting means for encrypting the web page further comprises selecting a browser supported encryption algorithm for encrypting the web page.

15. The system recited in claim 11, wherein the caching means for caching the web page further comprises providing a remote cache location.
16. The system recited in claim 11, wherein one of the browser and the browser cache is password protected from unauthorized users.
17. The system recited in claim 11, wherein the encrypting means for encrypting the web page further comprises defining a path for storing the web page which directs the web page to memory locations for encrypted data.
18. The system recited in claim 11, wherein web page information that is cached and then paged is paged as encrypted web page information.
19. A data processing system for securing information stored on a browser cache, the system comprising:
- opening means for opening an application using a browser;
 - performing means for performing an application specific function on the application using the browser, wherein application specific information is produced;
 - encrypting means for encrypting the application specific information; and
 - caching means for caching the application specific information.
20. A data processing system for securing information stored in a browser cache associated with a browser, the system comprising:

initiating means for initiating a session;
decrypting means for decrypting data contained in the browser cache, wherein the
decrypted data is associated with information content stored in the browser cache;
requesting means for requesting information stored in the browser cache;
checking means for checking the decrypting data for requested information; and
decrypting means for decrypting additional data contained in the browser cache, wherein
the decrypted data is the requested information.

21. A computer program product on a computer readable medium for securing information
stored in a browser cache associated with a browser comprising:

initiating instructions for initiating a session;
requesting instructions for requesting a first web page;
receiving instructions for receiving the web page;
encrypting instructions for encrypting the web page; and
caching instructions for caching the web page.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.